PERSONALLY IDENTIFIABLE INFORMATION (PII) BRIEFING

Key Issue:

- The continued loss of PII is placing our Soldiers in jeopardy.

Other issues:

- Sensitive Data is being lost
  - Found by those hostile to our way of life
- FOUO Data leaving the installations is making it's way to the public & others.

ALARACT 147/2007

- ARMY PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) AWARENESS
- REQUIREMENTS ALREADY EXIST, are not being met
- Commanders/Directors accountable
- Requirements (long list) must be met and reported NLT 27 JULY 2007

(NLT 1 Aug07 to HQDA)

PERSONALLY IDENTIFIABLE INFORMATION (PII) AWARENESS

JRTC & FT. Polk Commanders &Directors:

- WILL HAVE THEIR ORGANIZATIONS COMPLETE THE TASKS LISTED IN PARAGRAPH 3 of ALARACT 147/2007
- REPORT COMPLIANCE: Brigades & Directorates consolidate and send one report to DOIM) NLT 1200hrs 27 Jul 2007 (HQDA deadline 1Aug07)
- REQUIREMENT APPLIES TO SOLDIERS, DA CIVILIANS AND ARMY CONTRACTORS ON THE INSTALLATION.

Briefing END

- End of: PII “Briefing in a Nutshell”
- Specific, Tasks Follow
- Details to follow in OPORD
  - *(not produced as of 9JUL07 1500hrs)*

TASKS

- COMPLY WITH DAR MESSAGE (REFERENCE C) AND ARMY ACCELERATED IMPLEMENTATION OF COMMON ACCESS CARD CRYPTOGRAPHIC NETWORK LOGON (REFERENCE G)

- ENSURE ALL HIGH RISK MOBILE INFORMATION SYSTEMS AUTHORIZED FOR TRAVEL (I.E. LAPTOPS AND REMOVABLE STORAGE DEVICES SUCH AS THUMBDRIVES) ARE IDENTIFIED AND APPROPRIATELY CONFIGURED AND LABELED.

TASKS

- ENSURE LAPTOPS AUTHORIZED FOR TRAVEL ARE PROPERLY CONFIGURED FOR ENCRYPTING DATA AT REST USING AN ARMY APPROVED DAR SOLUTION OR IAW THE BEST BUSINESS PRACTICES IDENTIFIED IN REF E.
- 3.1.3 IAW REF G, THESE LAPTOPS WILL BE REQUIRED TO USE CAC CRYPTOGRAPHIC LOGON (CCL) FOR WINDOWS DOMAIN LOGON THROUGH GROUP POLICY OBJECT (MACHINE-BASED) ENFORCEMENT TO ELIMINATE THE USE OF USERID/PASSWORD AS A MEANS FOR DEVICE OR NETWORK ACCESS. THE USE OF CAC/PKI FOR ACCESS CONTROL COMBINED WITH ENCRYPTION OF DATA AT REST PROVIDES STRONG PROTECTION OF PII AND SENSITIVE DATA ON HIGH RISK MOBILE DEVICES.

TASKS

- 3.1.4 LABELS ON LAPTOPS MUST STATE THAT THE SYSTEM IS PROTECTED BY A DAR SOLUTION AND AUTHORIZED FOR TRAVEL IAW ALARACT MESSAGE DATED 271600Z OCT 06 SUBJECT: ARMY DATA-AT-REST (DAR) PROTECTION STRATEGY.

- LABELING ALSO APPLIES TO REMOVEABLE STORAGE DEVICES SUCH AS THUMBDRIVES IF THE DAR SOLUTION SUPPORTS REMOVEABLE MEDIA.

- ADDITIONALLY, PERSONALLY OWNED THUMBDRIVES THAT ARE USED IN AND AROUND THE GOVERNMENT WORKSPACE, WILL BE PROHIBITED OR LABELED AS *PERSONAL* AND WILL NOT BE USED FOR STORING ANY GOVERNMENT DATA OR PII.

TASKS

- LAPTOPS NOT IN FULL COMPLIANCE WILL NOT HAVE THE DAR LABEL AFFIXED AND ARE NOT AUTHORIZED FOR TRAVEL.

- ENSURE TRAVELERS ARE TRAINED ON PROCEDURES TO ENCRYPT AND DECRYPT SENSITIVE DATA USING ARMY APPROVED SOLUTIONS.

TASKS

- FOR ORGANIZATIONS WITH AN EXISTING DAR ENCRYPTION CAPABILITY, EXTEND WITHIN THE LIMITS OF CURRENT RESOURCES THOSE CAPABILITIES TO ALL REMAINING INFORMATION SYSTEMS WHERE DATA IS AT RISK.
  ORGANIZATIONS ARE NOT TO EXPEND RESOURCES IN ACQUIRING ADDITIONAL LICENSES TO COVER UNPROTECTED SYSTEMS. THE ARMY, ALONG WITH DOD AND OTHER FEDERAL AGENCIES PARTICIPATED IN A FEDERAL GOVERNMENT WIDE DAR ENCRYPTION ACQUISITION WHICH YIELDED MULTIPLE ENCRYPTION PRODUCTS.
  THE ARMY IS FINALIZING ITS DAR PROCUREMENT STRATEGY AND WILL RELEASE UPDATED POLICY THAT WILL IDENTIFY THE APPROVED PRODUCT(S) FOR USE BY ALL ARMY ACTIVITIES IN THE NEAR FUTURE.

TASKS

- ALL ASSIGNED PERSONNEL WILL COMPLETE THE ARMY G3 COMPUTER SECURITY TRAINING AND THE PROTECTION OF EXTERNAL REMOVABLE MEDIA TRAINING PACKAGES ARE LOCATED AT THE ARMY'S VIRTUAL INFORMATION ASSURANCE TRAINING URL HTTPS://IATRAINING.US.ARMY.MIL;

  LOG IN OR REGISTER AND THEN CLICK LESSON OPTIONS/SELECT MODULE AND SELECT THUMB DRIVE AWARENESS OR ARMY G3 COMPUTER SECURITY TRAINING.

TASKS

- ESTABLISH A SYSTEM TO REVIEW NEW MOBILE/LAPTOPS THAT ENTER THE UNITS INVENTORY FOR AN "AUTHORIZATION TO TRAVEL" STATUS AND APPLICABLE MARKINGS THAT A DAR SOLUTION WAS APPLIED AND IS USED TO ENCRYPT FOUO AND PII INFORMATION.